Identity Theft:
How It Happens, Its Impact on Victims, and Legislative Solutions

Beth Givens
Privacy Rights Clearinghouse
1717 Kettner Ave. Suite 105
San Diego, CA 92101
Voice: (619) 298-3396
Fax: (619) 298-5681
E-mail: prc@privacyrights.org
http://www.privacyrights.org

July 2000 (adapted from August 1999 presentation)

The Privacy Rights Clearinghouse is a nonprofit consumer information and advocacy program based in San Diego, California. The PRC was established in 1992. We have been assisting victims of identity theft since 1993, when we first started learning about this crime.

The following information is adapted from a presentation to the National Organization for Victim Assistance conference in August 1999. It is in four parts.

- Topic number one is the crime itself – what is identity theft, how much of it is going on, and why is it happening in epidemic proportions.

- Second, I will discuss the various ways in which identity thieves obtain the bits and pieces of information which they need to impersonate others -- mainly SSNs, credit card numbers and driver's license numbers.

- Third, I will explain some of the impacts on victims.

- And fourth, I will summarize legislative efforts to address identity theft.

First, what is identity theft? There are numerous variations of this crime. Essentially, it occurs when someone uses bits and pieces of information about an individual -- usually the Social Security number -- to represent him or herself as that person for fraudulent purposes. Examples are obtaining credit cards and loans in someone else's name and then not paying the bills, opening utility accounts, renting an apartment, getting a cellular phone, purchasing a car or a home, and so on. Another type of identity theft – what I call the worst case scenario – is when the perpetrator commits crime in the victim's name and gives that person a criminal record.

Victims are not liable for the bills accumulated up by the imposters, thanks to federal law. But they do have the anxiety and hassle of spending months, even years, regaining their financial health and restoring their good credit history.

How many victims of this crime are there? We don't have accurate statistics. But I estimate that there are 500,000 to 700,000 victims a year and rising. You can see a dramatic graph of the increase of the crime in recent years on the back of the Resources handout. This is from a federal government report. [U.S. Government Accounting Office, www.gao.gov, "Identity Fraud," 1998, p. 40, Report No. GGD-98-100BR] It shows a 16-fold increase from 1992 to 1997. The statistics are provided by the credit reporting bureau Trans Union which is currently receiving over 2,000 calls a day from victims of identity theft.

The three credit bureaus are Trans Union, Equifax, and Experian, formerly TRW. They each maintain a fraud department. When someone learns they are a victim of this crime, the first step they need to take is to contact these three bureaus and place a fraud alert on their file. If the imposter attempts to obtain additional credit in their name, the fraud alert is supposed to stop them, although this measure is not 100% effective.

Why is this crime so rampant today? I place a great deal of the blame on the credit industry. Credit grantors make it all too easy to obtain credit. They do not adequately check the identities of applicants before granting credit. Instant credit opportunities are especially popular with identity thieves for this reason. Credit grantors are all too eager, in their competitive zeal, to get new customers. Many consumers receive several pre-approved offers of credit each week.

By the way, if you want to stop receiving these solicitations, there's a single toll free number you can call to place yourself on an opt-out list, 888-5OPTOUT.

Another reason why this crime is of epidemic proportions is that it is very easy for the criminals to obtain the information needed – in particular the Social Security number. Sloppy information handling by businesses is one reason such information is easy to come by – documents tossed in the trash without shredding them, computer files and personnel records easily obtained by dishonest employees and so on.

Another reason identity theft is rampant is that it does not yet get the attention of law enforcement that more violent crimes receive – like breaking and entering, mugging, robbery by gunpoint, bank thefts and the like. Many violent criminals are moving to identity theft because they know that law enforcement resources are not yet sufficient to investigate the majority of such crimes. Many organized crime rings are perpetrating identity theft.

Identity thieves are rarely apprehended and sentenced. If they are, penalties are minimal and rarely include jail time. Community service and parole are common.

Topic number two -- a run-down of some ways that identity thieves obtain identifying

information about their victims, typically Social Security numbers, which can be used to apply for credit and even order someone's credit report; credit card numbers; dates of birth; and driver's license numbers.

- One is the old fashioned way -- by stealing a wallet or purse. The thief either uses the information obtained or provides the contents to a crime ring.

- Fishing credit card slips and loan or credit applications from the trash, and unfortunately many businesses, banks, mortgage companies, and restaurants do not shred these documents.

- An inside job -- having access to a computer terminal that is connected to one of the credit reporting bureaus, looking for names similar to the thief's, or just looking for someone with good credit. Obviously what goes hand in hand with this type of access is the negligence of the company which is permitting such access in an unmonitored environment. "Insiders" have also used their access to personnel records to obtain Social Security numbers of identity theft victims.

  We learned of a case where a member of a Nigerian crime ring was employed temporarily at a very large corporation. He downloaded the employee list containing SSNs and then one by one the employees' identities were used for fraudulent purchases. The employees didn't know about it until they started sharing stories and learned that many of them had been hit. It wasn't until much later that the human resources department confessed that they had known about the theft, but they didn't want to tell the employees and cause them to panic.

- Sadly, relatives or friends, roommates, household workers like health care givers, spouses going through a divorce who have a grudge -- these people obtain their Social Security number, driver's license number, credit card numbers by having access to their personal effects. By the way, this may sound unbelievable, but we have found this to be more common than you would think.

- Mail theft is another way of obtaining identifying information. We urge people not to leave their paid bills out at the mailbox for the carrier to pick up. It's better to drop them off at the Post Office. There's also insider mail theft, where credit card mail is stolen from the mail processing areas by postal employees.

- Then there's the change of address routine. The thief fills out a change of address card so the victim's mail is diverted to the thief's drop box. The thief obtains bank statements and credit card bills, maybe pre-approved offers of credit containing the information necessary to impersonate the victim. The Postal Service has recently initiated changes to make this more difficult.

- Application fraud is another method. The imposter fills out a credit application -- perhaps a pre-approved offer of credit retrieved from the trash -- with the victim's name and identifying information and has it sent to another address. The major credit card issuers say they are now more wary of changes of address, but their efforts are not foolproof.

- The Internet is becoming a more popular resource for identity thieves. Yes, there are web sites that sell people's Social Security numbers. Take a look at www.infoseekers.com, for example.

- And there are many more schemes. Many victims with whom we've spoken haven't a clue as to how their identifying information was obtained by the imposter.

Added to this recipe for identity fraud is the fact that merchants, banks, auto dealerships and others often make it easy for identity thieves to do their mischief. When's the last time a store clerk actually examined your signature on the back of a credit card. A couple of years ago a San Diego TV reporter exposed a prominent medical laboratory that tossed medical records into its dumpsters unshredded. They contained full name, address, Social Security number and date of birth, as well as the diagnosis.

Banks still issue the last four digits of the SSN as the default PIN number for ATM cards and for telephone banking access. Many insurance companies use the SSN as the insurance account number and have it emblazoned on member cards which must be carried in the wallet. MediCare cards have the SSN on them. Most colleges and universities use the SSN as the student ID. It's on their cards, and grades are often posted by the SSN. In many states, not California, the SSN is the driver's license number. All these acts put consumers at risk.

Topic number three: What happens to the victims of these crimes? Even though each identity fraud case is different, what happens to the victims is, sadly, all too similar.

- They get little to no help from any of the authorities who issued the identifying information to them in the first place. This includes the Social Security Administration and the Department of Motor Vehicles, although the DMV is getting better.

.

- Law enforcement doesn't investigate many such crimes. There's just too much of this type of crime occurring for them to handle, although the financial fraud departments of many police departments are being expanded.

  Many police and sheriff's departments refuse to issue a police report to the victims, although the LA Sheriff's Department is an exception. Many victims find they need the police report to prove their innocence to the credit card companies and the check guarantee services.

- Many victims report they do not get effective help from the credit grantors, banks, and the

credit bureaus. They describe difficulty in reaching the credit bureaus, and tell how they are treated disbelievingly by some creditors. And they report that flagging their credit report for fraud doesn't always stop the imposter from obtaining more credit.

By the way, there are many tips that we can impart to you on how to reduce your chances of becoming a victim of this crime. The booklet *Privacy Piracy* goes into detail on these, so I won't dwell on them here. But the most important tip is to order your credit report once, and better, twice a year. If you are a victim, you will see evidence of it there (if it's credit related) and you can stop it early.

- Victims also have to put with abusive collection agencies -- who threaten them with, for example, having their houses taken away from them.

- Another experience of victims is that they have to spend a great deal of time cleaning up the mess. I've talked to many who are taking the day, or the week, off work so they can make the necessary phone calls, write the letters, get affidavits notarized and so on. And this all costs money as well. Many victims are saddled with this situation for years. I've heard four, five, up to 10 years.

- Victims are often scarred emotionally. They feel violated and helpless -- and very angry. I've heard people who've called the hotline use the word "rape" to describe how they feel. I've talked to many who are crying or close to it because they can't stop what's happening to them, and no one else will either. I've talked with elderly people who are scared of losing their life savings and their homes. In one day alone, I talked to two women, who sounded like otherwise very reasonable people, say they'd like to "kill" the perpetrator.

  It's little wonder that people feel violated, helpless and angry. Victims are unable to rent an apartment, get a job, get a mortgage, buy a car, because of someone else's bad credit history recorded on their credit report. Essentially the entire burden of this crime is placed on the shoulders of the victims.

- The worst case scenario is when the thief commits crimes in the victim's name. We learned of a case where the imposter was a major drug dealer, using the identity of a high-tech company president. This man travels out of the country often and has to carry a letter from law enforcement which explains he is not the drug dealer, because he gets pulled into secondary inspection every time he comes back to the U.S. Recently law enforcement from another state, who had not read the entry on the NCIC crime data base completely, entered his bedroom in the early morning hours and tried to arrest him at gunpoint. He was able to explain his way out of it, but it took some doing.

  Another case that came to the hotline was a Latino man, a U.S. citizen, who was visiting relatives in Tijuana, Mexico, across the border from San Diego. He was taken into

secondary inspection on his way back to San Diego. A search of his SSN showed he was wanted for some crime in the Bay area. He was transported from San Diego to San Francisco and put in jail. It took him 10 days before one of the officers believed him, took his fingerprints, as he had requested all along, and realized they had the wrong person.

- Another worst case scenario is when the impersonator is working under the victim's name and SSN and the earnings show on the victim's Social Security Administration account. We learned of such a case that had been going on for 10 years. The impersonator got the victim's birth certificate, a public record in California. And when the victim acquired a new SSN, the impersonator was able to obtain it shortly thereafter.

- Finally, in order for victims to extricate themselves from the identity theft mess they find themselves in, they have to be fairly savvy consumers. They must be assertive with the credit card, banking and credit reporting industries. They must be assertive with all kinds of other officials as well. I have talked with many consumers who really are not equipped to deal with the challenges that this crime brings to them -- people whose first language is not English, or people whose English language skills are such that they cannot communicate at the level of complexity that this problem requires; and those who are semi-literate or illiterate and can't write the necessary letters. Unfortunately, there just aren't enough consumer assistance offices to help these people.

The awareness of identity theft among consumers has skyrocketed in the last year -- primarily because of media coverage. I think consumers are becoming much more wary of giving out personal information and having it given out without their consent, especially on the Internet. These outcries by members of the public have resulted in some legislative attention brought to the issue.

Topic number 4: What legislative remedies have been enacted?

In 1998 Congress passed and the President signed the Identity Theft and Assumption Deterrence Act (18 USC 1028). It makes identity theft a federal felony – when someone knowingly uses the identification of another person with the intention to commit any unlawful activity under federal and state law. Violations of this Act are investigated by federal agencies like the U.S. Secret Service, the FBI, and the U.S. Postal Inspection Service. Such crimes are prosecuted by the U.S. Department of Justice. This new law allows for restitution for victims. And it established an identity theft clearinghouse within the Federal Trade Commission. They now have a toll-free number for consumers to call, and a special section of their web site devoted to identity theft. [877-FTC-HELP] [www.ftc.gov/bcp/conline/edcams/identity/index.html]

In recent years approximately half the states criminalized identity theft. Most of them have made it a felony.

On the one hand, I'm pleased that this crime is being criminalized by these new laws. But I think

that in order to make a dent in identity theft, the practices of the credit industry must change dramatically. In fact, this crime is at epidemic proportions *primarily because* of the careless practices of the credit granting and the credit reporting industries. Until laws create incentives for the credit industry to change how they do business, the crime of identity theft will continue to climb at epidemic proportions.

Here are some suggestions for making credit industry practices more fraud proof:

- Require the credit grantor to verify at least four pieces of information -- name, address, date of birth, SSN, driver's license number, and place of employment -- with information on the credit report. This is especially important in instant credit situations. If the consumer is applying in person, the credit grantor must inspect a photo ID.

- If the credit grantor is offering credit via a mailed-in application -- in other words, a pre-approved offer of credit -- then the credit grantor should use the consumer's address as it appeared on the original solicitation, not a different address, which could well be the work of an identity thief. Further, if the card issuer receives a change of address notification, it also must send a confirmation notice to the address which it has on file.

- A stiff penalty should be assessed whenever a credit grantor extends credit to an imposter *after* the victim has placed a fraud alert on the credit file.

- All consumers should be able to receive one free copy of their credit report annually. Only six states have passed such laws: Colorado, Georgia, Massachusetts, Maryland, New Jersey, Vermont. With more consumers checking their credit reports more frequently, identity theft will be detected earlier and the impact will be minimized.

- Consumers should be able to notify the credit bureaus to in effect put a freeze on their credit report -- to prevent their credit report from being furnished without specifically authorizing the release.

- Another important piece of legislation that needs to be enacted is a provision that takes the Social Security number out of circulation.

That concludes my presentation.